Round skips for Poseidon

Àlex Rodríguez García[1]

[1]ETH Zurich, Switzerland

SPRING - CAHF
10/05/2026

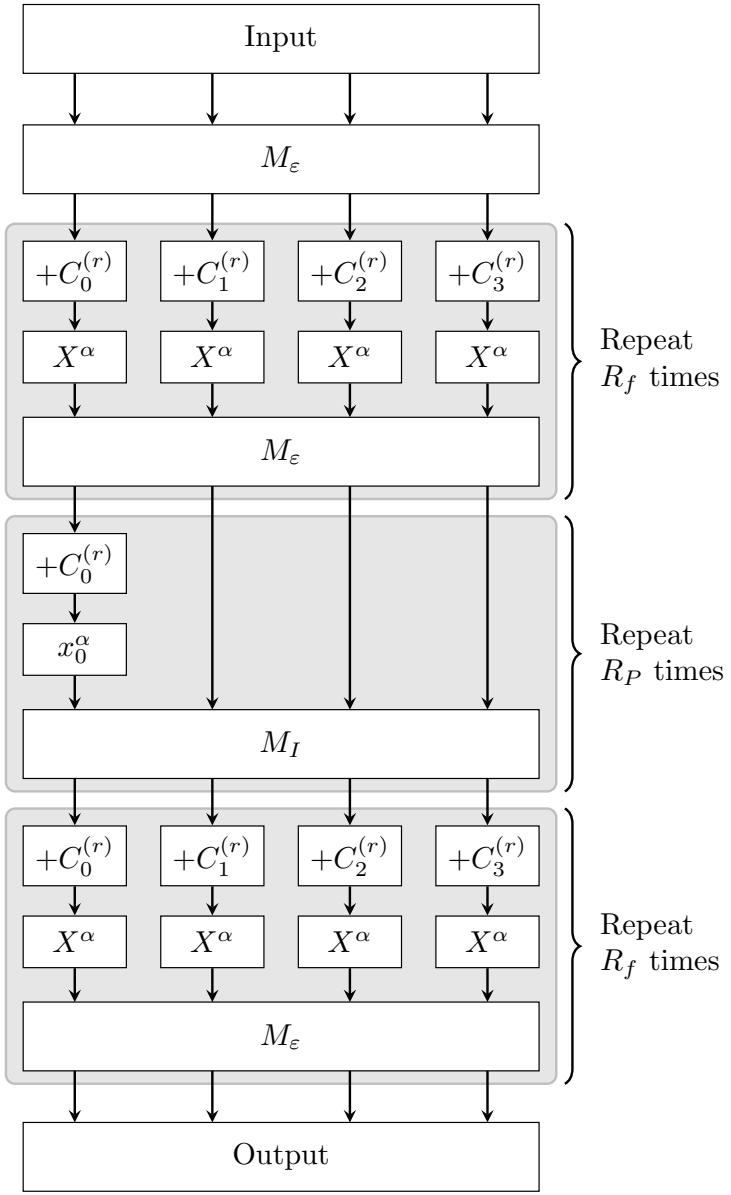
Main take-aways

- Poseidon and its variants are secure against the naive algebraic model.
- Using Poseidon with an initial linear layer makes sense, even if the original paper did not include it.
- MDS matrices are a secure choice for Poseidon.

Outline

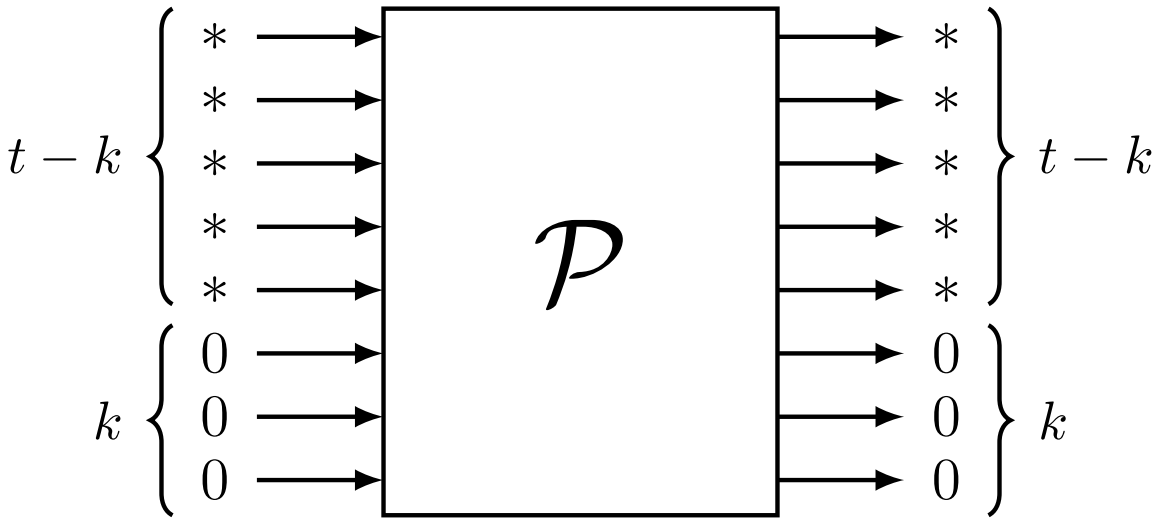
Poseidon2's design

- Permutation over t field elements.
- Used in sponge or compression mode.
- For this presentation, assume $p \approx 2^{31}$, $t \in \{16, 24\}$.



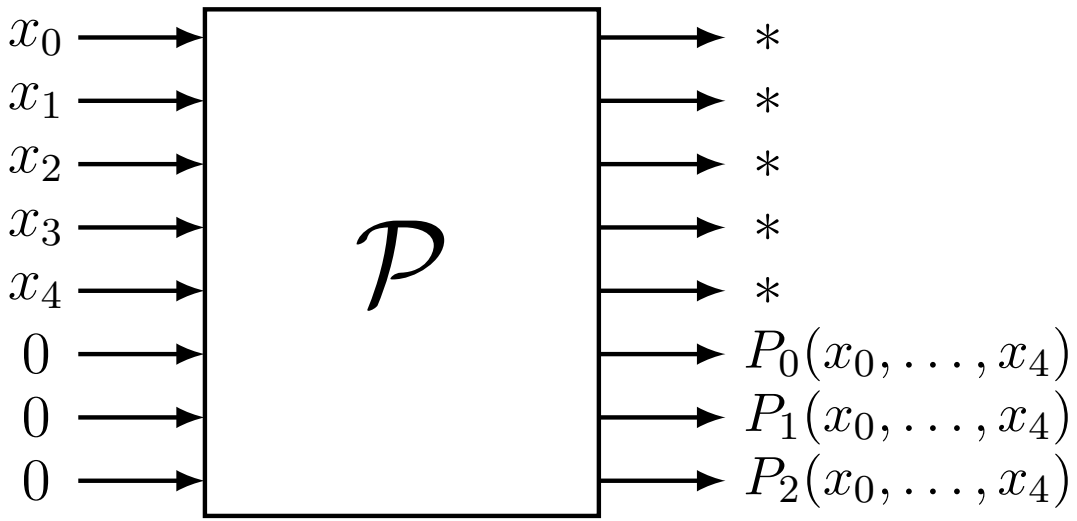
CICO problem

- Algebraic attacks against Poseidon are ususally benchmarked using the CICO-k problem.



Algebraic modeling (I)

- Model the input as variables, and the output as polynomials in these variables.
- Example with $t = 8$, $k = 3$:



Algebraic modeling (II)

- Solving the CICO-k problem is equivalent to finding a solution to the system:

$$P_0(x_0, x_1, x_2, x_3, x_4) = 0$$
$$P_1(x_0, x_1, x_2, x_3, x_4) = 0$$
$$P_2(x_0, x_1, x_2, x_3, x_4) = 0$$

- R rounds, power map x^α, multidegree of P_i is α^R.
- Usually, $\alpha = 3, 5$ or 7.
- Higher degrees make the system harder.

Why round skips?

- Lower the degree of the equations.
- Proven powerful: they were the main cause why Poseidon2 was discarded for lean Ethereum.

MDS matrix

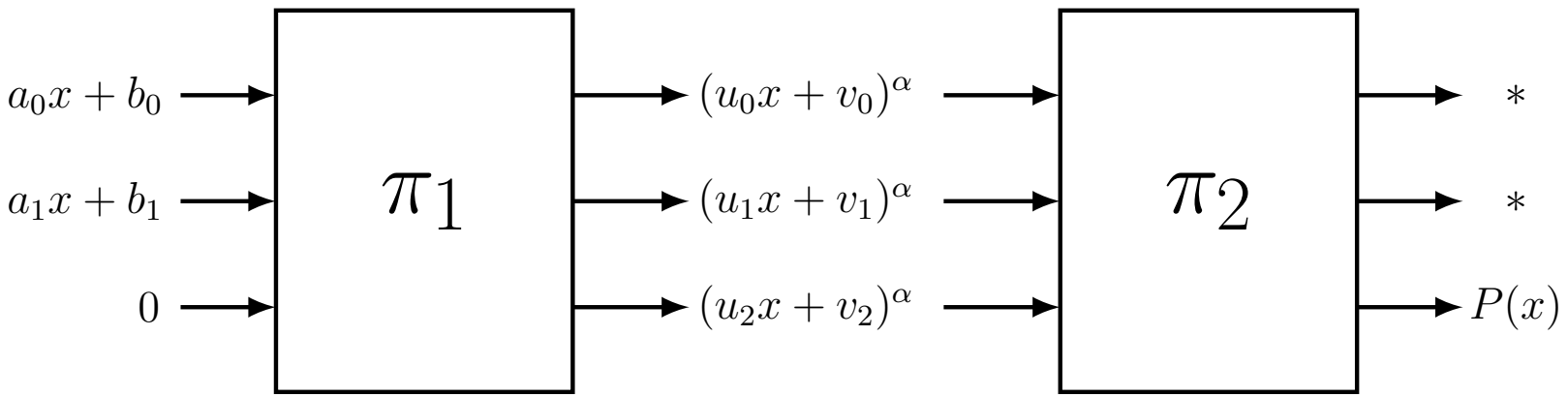
- Definition: a $t \times t$ matrix $\mathcal{M}$ is called MDS iff every $\ell \times \ell$ submatrix is full-rank, for all ℓ.
- Intuition: if $x \in \mathbb{F}^t \backslash \{0\}$, the number of zeroes in x and $\mathcal{M}x$ is at most $t - 1$.

Disclaimers and intuition

- This is how I understand the round skip intuitively, not how it was exposed in the original article.
- The original paper targets the original Poseidon design. Here, we assume there is a linear layer at the beginning.
- Intuition: linearize the first round to lower the degree of the output polynomials.

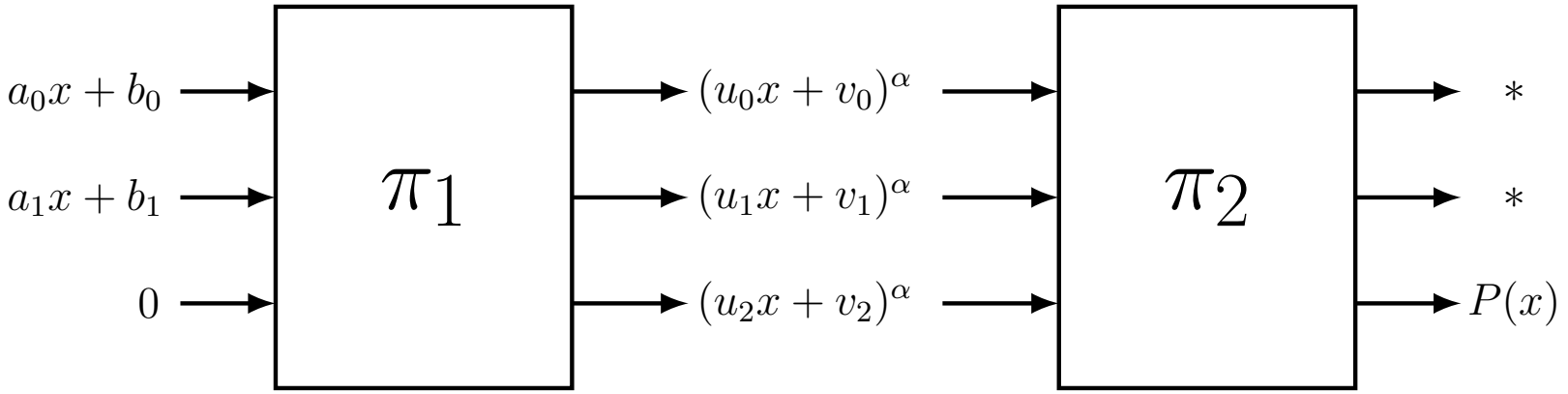
Round skip trick [BBLP22]

- $\pi_1 = \mathcal{S} \circ \mathcal{C} \circ \mathcal{M}$: Matrix multiplication, constant addition and power map $S(X) = X^\alpha$.



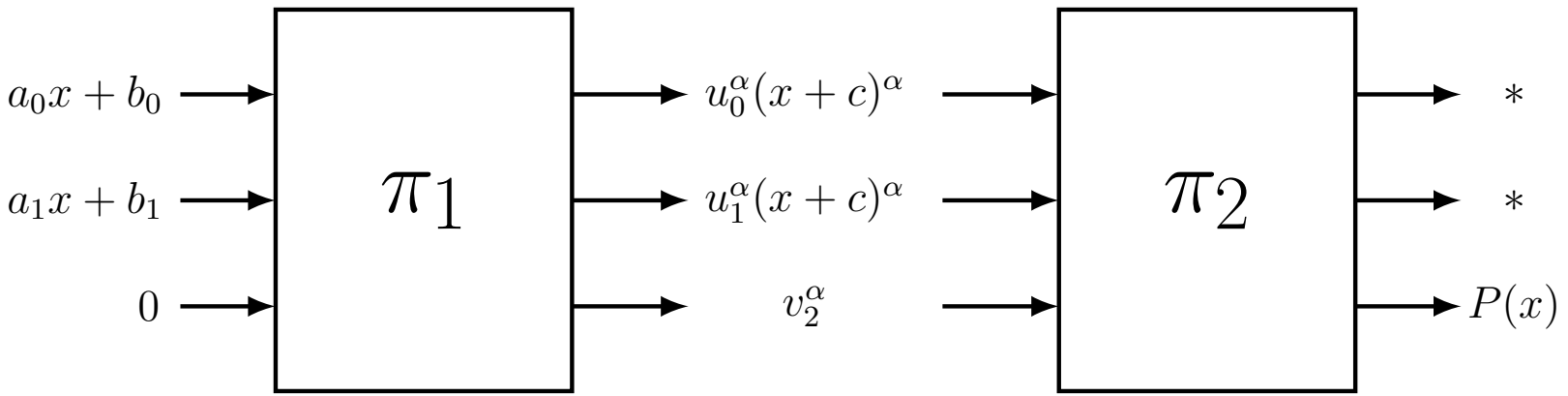
Round skip trick [BBLP22]

- u_i depends on a_j and the matrix, v_i depends on b_j, the matrix and round constants.
- We can choose a_j such that $u_2 = 0$, that determines u_0, u_1, both different from 0 (MDS property).
- We can choose b_j such that $u_1 v_0 = u_0 v_1$, or $c := v_0/u_0 = v_1/u_1$.



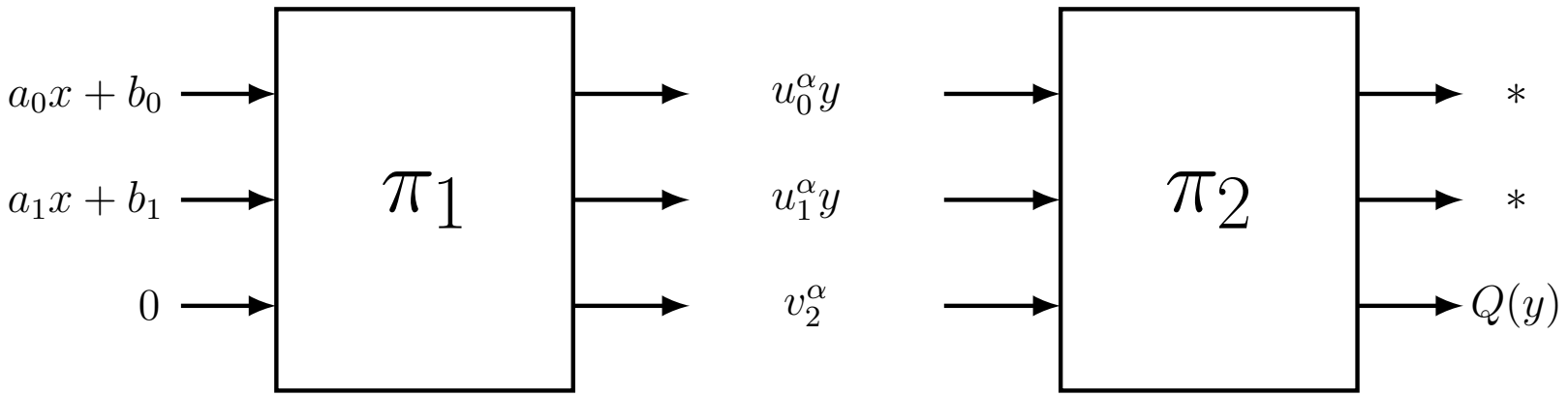
Round skip trick [BBLP22]

- u_i depends on a_j and the matrix, v_i depends on b_j, the matrix and round constants.
- We can choose a_j such that $u_2 = 0$, that determines u_0, u_1, both different from 0 (MDS property).
- We can choose b_j such that $u_1 v_0 = u_0 v_1$, or $c := v_0/u_0 = v_1/u_1$.



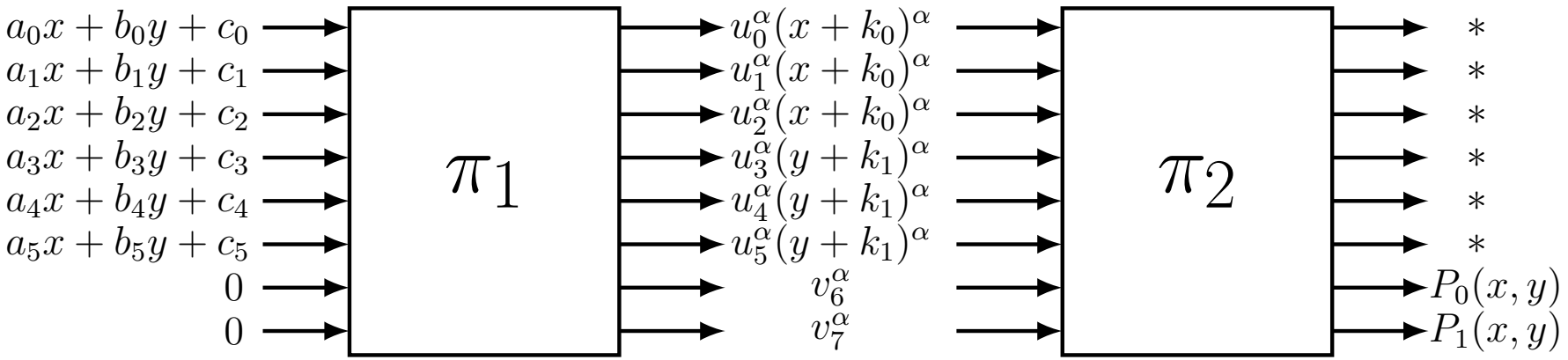
Round skip trick [BBLP22]

- We can do a change of variables! $(x+c)^\alpha = y$.
- $P(x)$ is a polynomial of degree α^R.
- $Q(x)$ is a polynomial of degree α^{R-1}.



Generalization

- For an MDS matrix, we can always make $\lfloor t/k \rfloor - 2$ change of variables.



Change in the linear layer

- Motivation: using Poseidon with smaller fields, the cost of matrix multiplications becomes a problem.
- The authors of Poseidon introduced a more efficient matrix:

$$M_\varepsilon := \begin{bmatrix} 2M & M & M & M \\ M & 2M & M & M \\ M & M & 2M & M \\ M & M & M & 2M \end{bmatrix}$$

- Clearly, non-MDS:

$$\begin{bmatrix} 2M & M & M & M \\ M & 2M & M & M \\ M & M & 2M & M \\ M & M & M & 2M \end{bmatrix} \begin{bmatrix} 0 \\ X \\ -X \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ MX \\ -MX \\ 0 \end{bmatrix}$$

Bounty instance example

- Biggest bounty instance in the Ethereum Poseidon Initiative 2025.
- $t = 16$, $p = 2^{31} - 1$, $k = 2$, power map x^5.
- Permutation consisting of:
  1. 3 external rounds
  2. 4 partial rounds
  3. 3 external rounds
- We describe a round skip exploiting the structure of the external layer.

Round skip (I)

- Input has 16 field elements. 2 forced to be 0, 4 are variables, 10 are constants.

$$X = (x_0, x_1, x_2, x_3)^T, \quad U_3^{(0)} = (u_8, u_9, 0, 0)^T$$

- $L_i(U^{(0)})$ represents a linear combination of $MU_j^{(0)}$.

$$\begin{bmatrix} U_0^{(0)} \\ U_1^{(0)} + X \\ -X \\ U_3^{(0)} \end{bmatrix} \xrightarrow{\mathcal{E}_0} \begin{bmatrix} (L_0(U^{(0)}) + C_0^{(0)})^5 \\ (MX + L_1(U^{(0)}) + C_1^{(0)})^5 \\ (-MX + L_2(U^{(0)}) + C_2^{(0)})^5 \\ (L_3(U^{(0)}) + C_3^{(0)})^5 \end{bmatrix}$$

Round skip (I)

- Input has 16 field elements. 2 forced to be 0, 4 are variables, 10 are constants.

$$X = (x_0, x_1, x_2, x_3)^T, \quad U_3^{(0)} = (u_8, u_9, 0, 0)^T$$

- $L_i(U^{(0)})$ represents a linear combination of $MU_j^{(0)}$.

$$\begin{bmatrix} U_0^{(0)} \\ U_1^{(0)} + X \\ -X \\ U_3^{(0)} \end{bmatrix} \xrightarrow{\mathcal{E}_0} \begin{bmatrix} (L_0(U^{(0)}) + C_0^{(0)})^5 \\ (MX + L_1(U^{(0)}) + C_1^{(0)})^5 \\ (-MX + L_2(U^{(0)}) + C_2^{(0)})^5 \\ (L_3(U^{(0)}) + C_3^{(0)})^5 \end{bmatrix} =: \begin{bmatrix} U_0^{(1)} \\ Y \\ -Y \\ U_3^{(1)} \end{bmatrix}$$

Round skip (II)

- $L_i(U^{(1)})$ represents a linear combination of $MU_j^{(1)}$.

$$\begin{bmatrix} U_0^{(1)} \\ Y \\ -Y \\ U_3^{(1)} \end{bmatrix} \xrightarrow{\mathcal{E}_1} \begin{bmatrix} (\quad L_0(U^{(1)}) + C_0^{(1)})^5 \\ (\quad MY + L_1(U^{(1)}) + C_1^{(1)})^5 \\ (-MY + L_2(U^{(1)}) + C_2^{(1)})^5 \\ (\quad L_3(U^{(1)}) + C_3^{(1)})^5 \end{bmatrix}$$

Round skip (II)

- $L_i(U^{(1)})$ represents a linear combination of $MU_j^{(1)}$.

$$\begin{bmatrix} U_0^{(1)} \\ Y \\ -Y \\ U_3^{(1)} \end{bmatrix} \xrightarrow{\mathcal{E}_1} \begin{bmatrix} (\quad L_0(U^{(1)})+C_0^{(1)})^5 \\ (\quad MY+L_1(U^{(1)})+C_1^{(1)})^5 \\ (-MY+L_2(U^{(1)})+C_2^{(1)})^5 \\ (\quad L_3(U^{(1)})+C_3^{(1)})^5 \end{bmatrix} =: \begin{bmatrix} U_0^{(2)} \\ Z \\ -Z \\ U_3^{(2)} \end{bmatrix}$$

Differences with previous round skips

- The change of variables is in blocks of 4 variables.

$$y_0 = (m_{00}x_0 + m_{01}x_1 + m_{02}x_2 + m_{03}x_3 + k_0)^5$$

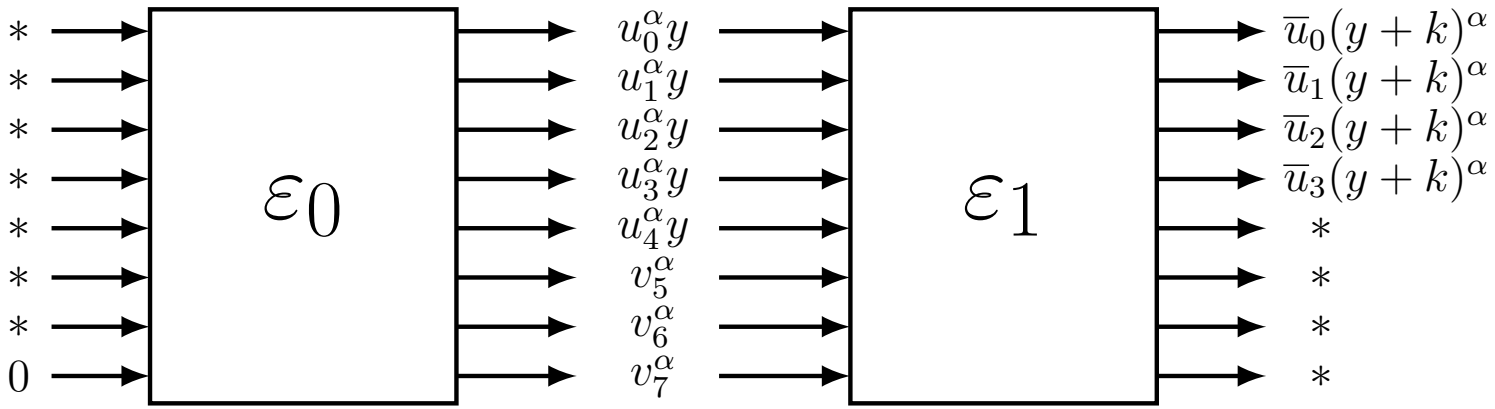
- Solution might not exist.

Recap

- For MDS matrices, if $x \in \mathbb{F}^t \backslash \{0\}$, the number of zeroes in x and $\mathcal{M}x$ is at most $t - 1$.
- Skipping rounds is doing changes of variables.
- For an MDS matrix, we can always make $\lfloor k/t \rfloor - 2$ change of variables (only the first round!).
- Can we improve that round skip to further rounds?

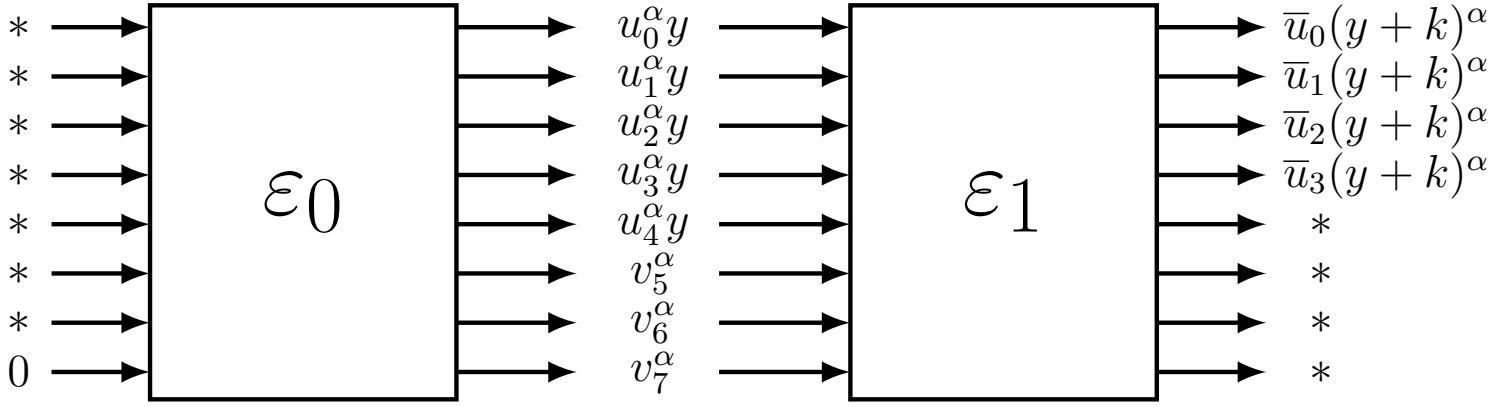
Security argument for MDS (informal)

- After one round skip $(x+c)^\alpha = y$, we have ℓ components that depend linearly on y, $t-\ell$ are independent of y.
- The next round, at least $t-\ell+1$ will depend on y.



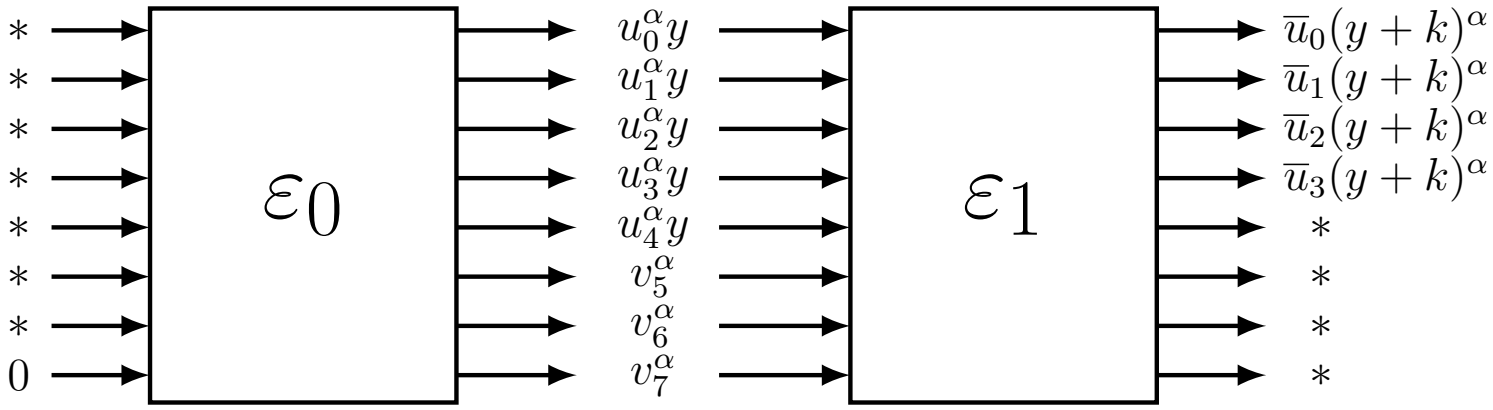
Security argument for MDS (informal)

- We need to impose $t - \ell$ equations: $k = \overline{v}_i / \overline{u}_i$.
- Therefore, the $t - \ell$ constants after the first round skip must be fixed!



Security argument for MDS (informal)

- We have $t-1$ degrees of freedom at the input, at most.
- 1 is used in x, $t-\ell$ in fixing v_i, $\ell-1$ in skipping x.



Summary of the presentation

- Revisit Poseidon design and algebraic modeling.
- Explore round skips in the literature.
- Describe attack improvements if the matrix is not MDS.
- Presented an informal (and incomplete!) security argument for the use of MDS matrices in Poseidon.

More about round skips: ia.cr/2026/306